



TOURO UNIVERSITY
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 33 | Number 3

Article 11

2017

iThink My Electronic Data Is Secure, but Is It: A Constitutional Analysis of in Re the Search of an Apple iPhone

Shira Bloom

Follow this and additional works at: <https://digitalcommons.tourolaw.edu/lawreview>



Part of the [Constitutional Law Commons](#), [First Amendment Commons](#), and the [Fourth Amendment Commons](#)

Recommended Citation

Bloom, Shira (2017) "iThink My Electronic Data Is Secure, but Is It: A Constitutional Analysis of in Re the Search of an Apple iPhone," *Touro Law Review*. Vol. 33: No. 3, Article 11.

Available at: <https://digitalcommons.tourolaw.edu/lawreview/vol33/iss3/11>

This Article is brought to you for free and open access by Digital Commons @ Touro Law Center. It has been accepted for inclusion in Touro Law Review by an authorized editor of Digital Commons @ Touro Law Center. For more information, please contact lross@tourolaw.edu.

iTHINK MY ELECTRONIC DATA IS SECURE, BUT IS IT? A CONSTITUTIONAL ANALYSIS OF *IN RE THE SEARCH OF AN APPLE iPHONE*

*Shira Bloom**

I. INTRODUCTION

The Constitutional *Right to Privacy* is a term that is commonly thrown around among American citizens and academics alike.¹ The issues that underlie this common phrase are disturbing to most: The United States Constitution provides a general right to privacy. The closest the Founding Fathers' document comes to addressing the issue of privacy is within the Fourth Amendment, which states:

[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.²

* Juris Doctor Candidate, May 2018; Bachelors of Arts in Political Science from the Lander College for Women, a division of Touro College. This note would not have been possible without my sister, Deena; you are my role model when it comes to selflessness and I could not have done this without you. To my father, Terrance, thank you for pushing me to be my best, while showing me unwavering support and encouragement. To my mother, Hilary, every success of mine belongs to you as well; thank you for being the greatest mom and always believing in me. Adi, Eitan, and my Bloom-Jackson-Kay-Schlosberg family: the loftier the building, the greater the foundation must have been laid; thank you for being so proud of my work, I would be nowhere without you. Professor C. Daniel Chill, thank you for being my mentor and for only being a phone-call away whenever I need advice, encouragement, or a good laugh. Cathy Breidenbach, your direction, patience, and commitment to perfection were my most valuable tools. Finally, thank you Professor Jeffery Morris for guiding me through this process and having confidence in my skills.

¹ Warren & Brandeis, *The Right to Privacy*, 5 HARV. L. REV. 148 (1891).

² U.S. CONST. amend. IV.

The underlying goal of this provision is to protect American citizens' privacy and freedom from arbitrary governmental intrusions.³ States are bound by the Fourth Amendment's provision that prevents arbitrary governmental intrusions through the Due Process Clause of the Fourteenth Amendment which applies the Constitution to the States.⁴ The relevant portion of the Fourteenth Amendment states, "no state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law"⁵ In addition, the Fourth Amendment requires the Government to acquire a warrant before engaging in the search of a private individual, or otherwise threaten to violate both the Fourth and Fourteenth Amendments.⁶ This is a valuable mechanism aimed to prevent unreasonable governmental interference.⁷

At the same time, the First Amendment of the Constitution provides that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech"⁸ Moreover, as the Second Circuit concluded in *Ford Motor Co. v. Lane*⁹ and *Universal City Studios, Inc. v. Corley*,¹⁰ computer code qualifies as speech and is subject to First Amendment protections.¹¹ As such, claims of interference of one's privacy rights have been raised with respect to smartphones, which have become increasingly popular among American citizens.¹²

The smartphone is a personal digital assistant that to many serves as an extension of the brain. The smartphone is home to personal thoughts, interactions, memories, and experiences that cannot

³ Scott E. Sundby, "Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?", 94 COLUM. L. REV. 1751, 1809-10 (1994).

⁴ Paul Finkelman, *John Bingham and the Background to the Fourteenth Amendment*, 36 AKRON L. REV. 671, 671-73 (2003) (noting the amendment was bitterly contested by the states which were forced to ratify it in order to regain representation in Congress).

⁵ U.S. CONST. amend. XIV, § 1.

⁶ *The Warrant Requirement*, *Georgetown Law Journal Annual Review of Criminal Procedure*, 44 GEO. L.J. ANN. REV. CRIM. PROC. 24, 25-32 (2015).

⁷ *Id.*

⁸ U.S. CONST. amend. I.

⁹ 67 F. Supp. 2d 745 (E.D. Mich. 1999).

¹⁰ 273 F.3d 429 (2d Cir. 2001).

¹¹ *Ford Motor Co.*, 67 F. Supp. 2d at 751; *Universal City Studios, Inc.*, 273 F.3d at 446-60.

¹² Lulu Chang, *Smartphone Usage Soars in US as other Device Popularity Declines*, DIGITAL TRENDS (Oct. 29 2015), <http://www.digitaltrends.com/mobile/us-smartphone-usage-soars/>.

be compared to any of its electronic predecessors.¹³ The smartphone keeps track of the location of its owner, the frequency of whom its owner communicates with, and the favorite applications of its owner.¹⁴ Thus, allowing the Government to have unhindered access to the smartphones of its citizens essentially provides the Government with access into those same citizens' brains.

Following the horrific shootings that took place in San Bernardino, California, on December 2, 2015, the Federal Bureau of Investigation (hereinafter "FBI") sought to obtain encrypted information contained on the shooter's iPhone, in conjunction with its investigation.¹⁵ Apple did not voluntarily cooperate and, consequently, the FBI filed a motion in the United States District Court for the Central District of California, seeking to compel Apple, Inc. (hereinafter "Apple") to create and turn over software that would enable the FBI to sidestep the encryption of the iPhone used by shooter, Syed Rizwan Farook,¹⁶ because the Apple iPhone was locked through a user-determined, numeric passcode.¹⁷ The court granted the motion but Apple refused to comply with the order and, before the court reached a final decision, the FBI withdrew its motion because it located a group of hackers who were able to override the encryption and provide unobstructed access to the phone.¹⁸ This Note will analyze the underlying constitutional principles raised in this court's evaluation of the action, the strength of the Government's Application, and ultimately conclude that Apple should not have been required to turn over the software, because: (1) an individual's right to privacy with regard to a smartphone exists, and (2) speech in the form of computer

¹³ Yo Zushi, *Life with a Smartphone is Like Having a Second Brain in Your Pocket*, NEWSTATSMAN (Feb. 22, 2017), <http://www.newstatesman.com/science-tech/2017/02/life-smartphone-having-second-brain-your-pocket>.

¹⁴ Ben Patterson, *4 Ways Your Android Device is Tracking You (and How to Stop it)*, PC WORLD (April 13, 2015), <http://www.pcworld.com/article/2907061/4-ways-your-android-device-is-tracking-you-and-how-to-stop-it.html>; Charles Arthur, *iPhone Keeps Record of Everywhere You Go*, THE GUARDIAN (April 20, 2011), <https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears>.

¹⁵ Government's Ex Parte Application for Order Compelling Apple Inc., to Assist Agents in Search; Memorandum of Points and Authorities; Declaration of Christopher Pluhar; Exhibit at 9-17 In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter "*Ex Parte Application*"].

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

code should be afforded constitutional protection under the First Amendment.

II. CONSTITUTIONAL ISSUES

Two key constitutional issues are at stake in the *FBI v. Apple* case: the right to privacy and the protection of speech. The case precedent clearly indicates that Apple's conduct was justified by these constitutional provisions. The court should have granted Apple's motion to vacate the order which violated Apple's and its users' freedom from subjective governmental meddling and disturbed Apple's freedom of speech.

A. The Privacy Issue

By refusing to turn over the code, Apple protected its users' privacy. The Fourth Amendment prohibits the Government from engaging in unreasonable searches and seizures of persons or property.¹⁹ Here, the question is whether or not data should be treated as property and be subject to Fourth Amendment protection.²⁰ Although the FBI withdrew its motion, the faceoff between law enforcement and one of the world's largest technological companies remains largely unresolved.²¹ This case serves as a proxy for the larger pitted issue posed, which is whether society's demand for protection from crime and terrorism is greater than its legitimate desire to retain personal privacy in a purchaser's digital life.²²

Private companies want consumers to trust them with private information. At the same time, Congress has considered efforts to ensure that no company is exempt from complying with a court order, requiring the company to assist law enforcement, even if that means decrypting customer information.²³ These discussions have

¹⁹ U.S. CONST. amend. IV.

²⁰ U.S. CONST. amend. IV (noting that real property is protected by the Fourth Amendment's limitation on unreasonable search and seizure).

²¹ Mark Skilton, *What the Apple Versus FBI Debacle Taught Us*, SCIENTIFIC AMERICAN (May 20, 2016), <https://blogs.scientificamerican.com/guest-blog/what-the-apple-versus-fbi-debacle-taught-us/>.

²² Carrie Cordero & Marc Zwillinger, *Should Law Enforcement Have the Ability to Access Encrypted Communications?*, THE WALL STREET JOURNAL (April 19, 2015), <https://www.wsj.com/articles/should-law-enforcement-have-the-ability-to-access-encrypted-communications-1429499474>.

²³ *Id.*

encouraged companies, such as Facebook owned WhatsApp, to provide exhaustive military-strength message encryption for its 1 billion monthly active users.²⁴

The Government has also been accused of imposing a double standard based on the size of the company it is competing against.²⁵ For example, Edward Snowden, a former National Security Agency (hereinafter “NSA”) contractor, used Lavabit, a smaller tech startup company, to encrypt and host his email server.²⁶ Snowden discovered what the NSA was doing with personal data belonging to individuals and decided to expose it to the world, at the expense of his salary and freedom.²⁷ In June 2013, the FBI ordered Lavabit founder, Ladar Levinson, to turn over the encryption key so the Government could access Snowden’s emails.²⁸ Those keys also provided the Government unhindered access to 400,000 Lavabit users’ emails.²⁹ Thereafter, the Lavabit case proceeded under seal.³⁰

Conversely, Apple was able to withstand the FBI’s push for access to the encrypted information while Lavabit was not, in part, was due to the vast number of people who trust their Apple iPhones, and other Apple products, with their most intimate thoughts and expressions.³¹ Apple has been compared to a spiritual leader with a religious following, not just in North America, but all around the world.³² Indeed, millions of users follow the company with dedication that is akin to a cult.³³ Each time a new product is announced there is considerable excitement with consumers waiting in lines for hours, if

²⁴ Oana Ciobotea, *Why the Apple-FBI Battle Made People Realize the Importance of Privacy Faster Than Snowden*, VENTUREBEAT (April 29, 2016), <http://venturebeat.com/2016/04/29/why-the-apple-fbi-battle-made-people-realize-the-importance-of-privacy-faster-than-snowden/>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ Luke Harding, *How Edward Snowden went from Loyal NSA Contractor to Whistleblower*, THE GUARDIAN (Feb. 1, 2014), <https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract>.

²⁸ *Lavabit Founder Refused FBI Order TO Hand Over Email Encryption Keys*, THE GUARDIAN (Oct. 3, 2013), <https://www.theguardian.com/world/2013/oct/03/lavabit-ladar-levison-fbi-encryption-keys-snowden>.

²⁹ *Id.*

³⁰ Ciobotea, *supra* note 24.

³¹ Ciobotea, *supra* note 24.

³² Ciobotea, *supra* note 24. (explaining why the response to the privacy issues raised in the Apple v. FBI case were so much greater than with Lavabit and Snowden).

³³ Ciobotea, *supra* note 24.

not days, to get their hands on the latest products.³⁴ Therefore, when Apple is targeted in a legal action by the Government, citizens pay close attention to how the litigation unfolds.³⁵ People are interested in the future protection of their data from Government intrusion and it is likely that no users truly think that they are safe from intrusion and have nothing to hide.³⁶

Moreover, Lavabit was not afforded the opportunity to have a public trial and, thus, had to fight the battle against the Government alone and out of public view.³⁷ This left Lavabit without the support of other tech giants and privacy supporters, while also facing the threat of potential arrests, should it not comply with the Government's demands.³⁸ Lavabit ultimately shut down after complying and being forced to give in to the Government's requests.³⁹ Political analysts argue that fighting terrorism, at the cost of every citizen's privacy, is inherently wrong.⁴⁰

As the Supreme Court determined in *Katz v. United States*,⁴¹ the privacy right protected by the Fourth Amendment is a reasonable expectation of privacy.⁴² The test for a reasonable expectation of privacy is, "first that a person have exhibited an actual [subjective] expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"⁴³ However, the Fourth Amendment, cannot be translated into a general constitutional "right to privacy."⁴⁴

The strongest argument for preventing the Government from accessing the computer data is that the data should be treated as

³⁴ Katie Utehs, *People, Robot Wait in Line for New iPhone 6S in Palo Alto*, ABC 7 NEWS (Sept. 24, 2015), <http://abc7news.com/technology/people-robot-wait-in-line-for-new-iphone-6s-in-palo-alto-/1001082/> (noting that a woman waiting in line for Apple products in robot form); Chris Matyszczyk, *Yes, People are Already Lining up for iPhone 7*, CNET (Sept. 12, 2016), <https://www.cnet.com/news/yes-people-are-already-lining-up-for-iphone-7/>; Dave Smith, *I Spent 7 Grueling Hours in Line for an iPhone 7*, BUSINESS INSIDER (Sept. 19, 2016), <http://www.businessinsider.com/apple-iphone-7-launch-day-lines-photos-2016-9>.

³⁵ See Ciobotea, *supra* note 24 (explaining why the responses to the privacy issues raised in the Apple v. FBI case were so much greater than with Lavabit and Snowden).

³⁶ Ciobotea, *supra* note 24.

³⁷ Ciobotea, *supra* note 24.

³⁸ Ciobotea, *supra* note 24.

³⁹ Ciobotea, *supra* note 24.

⁴⁰ Ciobotea, *supra* note 24.

⁴¹ 389 U.S. 347 (1967).

⁴² *Id.* at 350.

⁴³ *Id.* at 360-61 (Harlan, J., concurring).

⁴⁴ *Id.* at 350.

property.⁴⁵ This issue is mostly discussed in the realm of insurance law and the labeling of computer data as tangible computer property.⁴⁶ In *Centennial Insurance Co. v. Applied Health Care System*,⁴⁷ a faulty server was installed, resulting in the loss of important files.⁴⁸ The insurer refused to defend the stolen property because of the inability to prove damage to tangible property.⁴⁹ The court held that the insurance company was required to defend the loss because it was possible for the plaintiff to prove that the loss was to tangible property.⁵⁰

Further, in *Retail Systems, Inc. v CNA Insurance Cos.*,⁵¹ a customer's computer tape suspiciously vanished while in the insured's custody.⁵² After finding the phrase "tangible property" to be ambiguous in the case of computer data, the court held that the data recorded on the tape was merged with the tape itself.⁵³ Therefore, when the entire tape was lost along with its embedded data, there had been a loss of tangible property.⁵⁴ However, the *Retail Systems* court did not actually answer the question of whether data itself, apart from the medium in which it is stored, is tangible property.⁵⁵ Therefore, the question of whether data is considered to be tangible personal property remains to be addressed by the courts and, if so, whether it implicates the right to privacy protected by the Fourth Amendment.⁵⁶

Commentators assert that legislation is necessary for anyone who believes personal data protection is "a fundamental civil liberty interest, essential to individual autonomy, dignity and freedom in a

⁴⁵ *Id.*

⁴⁶ Michael Rossi, *Is Computer Data "Tangible Property" or Subject to "Physical Loss or Damage"?—Part 1*, INTERNATIONAL RISK MANAGEMENT INSTITUTE, INC. (Aug. 2011), <https://www.irmi.com/articles/expert-commentary/is-computer-data-tangible-property-or-subject-to-physical-loss-or-damage-part-1>.

⁴⁷ 710 F.2d 1288 (7th Cir. 1983).

⁴⁸ *Id.* at 1290.

⁴⁹ *Id.* at 1291-92 (noting that only the duty to defend was at issue, the court stopped short of deciding that the computer data was in fact tangible property).

⁵⁰ *Id.* at 1292.

⁵¹ 469 N.W.2d 735 (Minn. Ct. App. 1991).

⁵² *Id.* at 736-37.

⁵³ *Id.* at 737-39.

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ Mark Skilton, *Is Personal Data the Same as Personal Property?*, THE HUFFINGTON POST (April 15, 2015), http://www.huffingtonpost.com/professor-mark-skilton/is-personal-data-the-same_b_9698952.html.

democratic civil society.”⁵⁷ Furthermore, a property rights model would establish the right to sell personal data and secure additional value in the marketplace and force companies to internalize costs resulting from the widespread collection and use of personal data.⁵⁸ Essentially, the Fourth Amendment combined with real property law would provide protection against certain unauthorized searches for the purpose of gaining access to information.⁵⁹ In addition, the Fifth and Fourteenth Amendment would provide protection against compulsion to reveal information.⁶⁰ In sum, the Government is able to create property rights when appropriate and, even though doing so is uncommon, the developments in the area of intellectual property may provide an impetus to do so.⁶¹

B. The Speech Issue

Apple’s computer code should also be protected under the First Amendment. The scope of First Amendment protection is largely dependent on whether a restriction is imposed because of the content of the speech.⁶² Content-based restrictions are permitted only if they serve a compelling state interest and do so by the least restrictive means available.⁶³ A restriction on neutral content is permitted if the restriction serves a substantial Government interest, the interest is unrelated to the censorship of free speech, and the regulation is narrowly tailored which, in the present framework, requires that the

⁵⁷ Paula Samuelson, *Privacy as Intellectual Property*, BERKELEY, http://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf (last visited Mar. 25, 2017).

⁵⁸ See Fair Credit Reporting Act, 15 U.S.C. § 1681 et. seq. (2017) (providing an overview of state and federal information privacy laws).

⁵⁹ Samuelson, *supra* note 57.

⁶⁰ See *Feist Pub., Inc. v. Rural Telephone Service Co.*, 499 U.S. 340 (1991) (holding copyright law does not confer exclusive rights in information in order to achieve constitutional purpose of promoting knowledge). Information can, sometimes be protected against unfair competition, including breaches of confidential relationships. See, *International News Service v. Associated Press*, 248 U.S. 215 (1918); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of The Public Domain*, 74 N.Y.U. L. REV. 354 (1999); L. Ray Patterson & Stanley F. Birch, Jr., *Copyright and Free Speech Rights*, 4 J. INTELL. PROP. L. 1 (1996); Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965 (1990).

⁶¹ See Margaret Jane Radin, *Property Evolving in Cyberspace*, 15 J.L. & COMM. 509, 511-13 (1996) (discussing utilitarian criteria for creation of property rights).

⁶² *Id.* at 514.

⁶³ Eugene Volokh, *Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny*, 144 U. PENN. L. REV. 2417 (1997).

means chosen do not place a more substantial burden on speech than is necessary to further the Government's legitimate interests.⁶⁴

The First Amendment protection afforded to computer code is an important and evolving concept relating to intellectual property.⁶⁵ The Second Circuit held in *Universal City Studios, Inc. v. Corley*⁶⁶ that regardless of source code and object code being written in an obscure manner and language, it still qualified as speech.⁶⁷ In *Universal City Studios, Inc.*, Universal City sought to enjoin Corley from posting code on its website that would override the encryption on digital disk (DVD) movies and thus provide unhindered access to the content.⁶⁸ The court discussed the scope of protection given to speech by the First Amendment and concluded, "dry information devoid of advocacy, political relevance or artistic expression was found to be accorded First Amendment protection."⁶⁹ In other words, computer software is not discharged from classification as First Amendment speech solely because reading the program requires the use of a machine or computer.⁷⁰ More succinctly, "[a] recipe is no less 'speech' because it calls for the use of an oven, and a musical score is no less 'speech' because it specifies performance on an electric guitar."⁷¹ What sets computer programs apart from conventional instructive language is that computer programs are executable on a computer.⁷² The datum that software has the capability to "direct the functioning of a computer does not mean that it lacks the additional capacity to convey information, and it is the conveying of information that renders instructions 'speech' for purposes of the First Amendment."⁷³ The communication transported by typical instructions is how to

⁶⁴ *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 450 (2d Cir. 2001).

⁶⁵ *Id.* at 435-37.

⁶⁶ *Id.*

⁶⁷ *Id.* at 436; See Daniel S. Lin et al., *Source Code Versus Object Code: Patent Implications for the Open Source Community*, 18 SANTA CLARA HIGH TECH. L.J. 235, 238-41 (2001) (stating that source code is a category of computer language instructions that is typically read and written by software programmers. The computer is unable to run the program on source code alone, and must convert it into object code. Object code contains numeric codes that inform the computer where to store information in the memory and instruct the computer how to act).

⁶⁸ *Universal City Studios, Inc.*, 273 F.2d at 436.

⁶⁹ *Id.* at 446.

⁷⁰ *Id.*

⁷¹ *Id.* at 447.

⁷² *Id.* at 447-49.

⁷³ *Universal City Studios, Inc.*, 273 F.3d at 447-49.

accomplish a task.⁷⁴ Thus, the Second Circuit held that the source code and object code were speech for First Amendment purposes.⁷⁵

Likewise, in *Junger v. Daley*,⁷⁶ the Sixth Circuit held that all source code is protected by the First Amendment because it serves to convey an idea relating to computer programming.⁷⁷ The plaintiff in this case was a professor who wished to share examples of source code on the internet to explain how encryption works.⁷⁸ He sued, claiming that the Export Administration Regulations that govern export of encryption software were unconstitutional.⁷⁹ The court held that source code is an expressive avenue to communicate ideas about computer programming and, accordingly, is protected by the First Amendment.⁸⁰ The *Junger* court determined that the general, expressive nature of source code deemed it protected speech, and further acknowledged that in some instances the Government has a legitimate interest in regulating source code.⁸¹ In its decision, the court reasoned that “all ideas having even the slightest redeeming social importance, including those concerning the advancement of truth, science, morality, and arts have the full protection of the First Amendment.”⁸² Although, source code cannot function until paired with an object code and executed on a computer, computer scientists still regard source code as a method of communication and expression.⁸³

Furthermore, software engineers refer to computer code as a language.⁸⁴ This verbiage, although not dispositive, leads one to equate computer code with expression much like speech, oral or written, which is what the language of the First Amendment protects.⁸⁵

⁷⁴ See *id.* at 451.

⁷⁵ *Id.* (holding that computer code combined speech with non-speech elements).

⁷⁶ 209 F.3d 481 (6th Cir. 2000).

⁷⁷ *Id.* at 484-85; *Recent Cases: Constitutional Law - Free Speech Clause - Sixth Circuit Classifies Computer Source Code as Protected Speech. - Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), 114 HARV. L. REV. 1813, 1813 (2001) [hereinafter “Recent Cases”].

⁷⁸ *Id.* at 1814.

⁷⁹ *Id.* at 1813-14.

⁸⁰ *Id.* at 1815.

⁸¹ See *Junger*, 209 F.3d at 485.

⁸² *Id.* at 484 (quoting *Roth v. United States*, 354 U.S. 476, 484 (1957)).

⁸³ *Id.* at 483.

⁸⁴ *Classifying Coding Languages*, LOYOLA MARYMOUNT UNIVERSITY LOS ANGELES, <http://cs.lmu.edu/~ray/notes/pltypes/> (last visited, Mar. 22, 2017) (coding languages vary and some examples include C++, C sharp, Raspberry Pie, etc).

⁸⁵ *Recent Cases*, *supra* note 77, at 1816-18.

Source code should be easy to read, understand, and modify by those familiar with it.⁸⁶ Most application software is distributed in a form that hides the source code, which is referred to as an executable file.⁸⁷ If the source code were to be included and easily accessible, the user would be able to modify or study the code and make substantial changes.⁸⁸ Software engineers often find it useful to analyze source code written by others to learn programming tools and techniques.⁸⁹

Another example of the Supreme Court's broadening application of the First Amendment, specifically through freedom of speech, is *United States v. O'Brien*.⁹⁰ In this 1968 Supreme Court case, the defendant was criminally convicted for burning his Selective Service registration certificate on the steps of a Boston Courthouse.⁹¹ At that time, when a male reached age 18, he was required to register with a local draft board pursuant to the Universal Military Training and Service Act.⁹² He was then assigned a Selective Service number and five days following the registration, he was issued a registration certificate and became eligible for induction.⁹³ O'Brien argued that the 1965 Amendment "prohibiting the knowing destruction or mutilation of certificates" was unconstitutional because "it was enacted to abridge free speech, and because it served no legitimate legislative purpose."⁹⁴ He further claimed that "the freedom of expression which the First Amendment guarantees includes all modes of 'communication of ideas by conduct,' and that his conduct is within this definition because he did it in 'demonstration against the war and against the draft.'"⁹⁵

The Court found that an important governmental interest exists when regulating a course of conduct that combines speech and non-speech elements in the same expression,⁹⁶ and that the governmental interest in regulating the non-speech component can rationalize

⁸⁶ Margaret Rouse, *Definition: Source Code*, TECH TARGET NETWORK (Nov. 2016), <http://searchmicroservices.techtarget.com/definition/source-code>.

⁸⁷ Daniel S. Lin et al., *supra* note 66, at 236-37.

⁸⁸ *Obligatory accreditation system for IT security products*, METAFILTER (Sept. 22, 2008), <http://www.metafilter.com/75061/Obligatory-accreditation-system-for-IT-security-products>.

⁸⁹ Rouse, *supra* note 86.

⁹⁰ 391 U.S. 367 (1968).

⁹¹ *Id.* at 369.

⁹² *Id.* at 372.

⁹³ *Id.* at 372-73.

⁹⁴ *Id.* at 370.

⁹⁵ *O'Brien*, 391 U.S. at 376.

⁹⁶ *Id.* at 376-77.

accompanying limitations on First Amendment freedoms.⁹⁷ In reaching its decision, the Court reasoned that to characterize the importance of the governmental interest which must exist, “the Court has employed a variety of descriptive terms: compelling; substantial; subordinating; paramount; cogent; strong.”⁹⁸ The Court in *O’Brien* went on to state that a Government regulation is constitutionally justified so long as it “furthers an important or substantial governmental interest . . . the governmental interest is unrelated to the suppression of free expression; and . . . the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest,” essentially a strict scrutiny analysis.⁹⁹ In addition, when a Court conducts its evaluation, it weighs the state’s interests against the speaker’s interests.¹⁰⁰ In *O’Brien*, the Court ultimately found that the Military Training and Service Act was constitutional and satisfied all of the requirements of the First Amendment articulated by the court.¹⁰¹ Consequently, the First Amendment did not protect O’Brien’s actions of burning the certificate.¹⁰²

Justice Harlan, concurring with the majority opinion, stated that O’Brien’s actions satisfied the Court’s test and, moreover, that O’Brien could have communicated his message in other lawful ways, rather than burning his draft card.¹⁰³ Justice Harlan pointed out that the majority relied on the governmental interest test but continued by stating that this test does not bar constitutional challenges on First Amendment grounds in the rare circumstances that “an ‘incidental’ restriction upon expression . . . satisfies the Court’s other criteria, [yet] in practice has the effect of entirely preventing a ‘speaker’ from reaching a significant audience with whom he could not otherwise lawfully communicate.”¹⁰⁴

A very different issue was raised in *In Re The Search of Apple iPhone*.¹⁰⁵ Specifically, the question before the court was whether the

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *O’Brien*, 391 U.S. 367 at 380-82.

¹⁰¹ *Id.* at 388.

¹⁰² *Id.*

¹⁰³ *Id.* at 388-89.

¹⁰⁴ *Id.*

¹⁰⁵ See generally Order Compelling Apple, Inc. to Assist Agents in Search, *In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus*

right to refrain from speaking is protected under the First Amendment.¹⁰⁶ This question was recently decided in the affirmative in the 2016 California Court of Appeals for the Second District's decision, *Suarez v. Trigg Laboratories, Inc.*¹⁰⁷ Here, the California court held that the right to freedom of speech provided by the First Amendment encompassed what a speaker chooses to say, and what a speaker chooses not to say; it is a right to speak freely and also a right to refrain from speaking altogether.¹⁰⁸ This concept dates back to 1943, when the Supreme Court held that "a system which secures the right to proselytize religious, political, and ideological causes must also guarantee the concomitant right to decline to foster such concepts. The right to speak and the right to refrain from speaking are complementary components of the broader concept of 'individual freedom of mind.'"¹⁰⁹ This concept must now be applied to the *Apple* case and whether a court may compel that source code be written to assist the Government in a criminal investigation.

III. THE FBI V. APPLE

Apple's right to privacy concerns and its need for First Amendment protections clashed with the FBI's need to investigate a serious crime in *In Re The Search of an Apple iPhone*. The FBI believed that the prevention of homegrown terrorists from conducting acts of terrorism outweighed any interest Apple has in protecting the data of its users. Apple believed that the company's constitutional interests were compelling and deserved protection from the FBI.

A. *In Re The Search of An Apple iPhone*

As part of the investigation into the San Bernardino massacre, the United States filed an *ex parte* application for an order compelling

IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter "*Order Compelling*"].

¹⁰⁶ Apple Inc.'s Motion to Vacate Order Compelling Apple, Inc. to Assist Agents in Search and Oppositions to Government's Motion to Compel Assistance at 33, *In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300*, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter "*Motion to Vacate*"].

¹⁰⁷ 3 Cal. App. 5th 118 (Cal. Ct. App. 2016).

¹⁰⁸ *Id.* at 124.

¹⁰⁹ *Wooley v. Maynard*, 430 U.S. 705, 714 (1977); *West Virginia State Bd. of Educ. v. Barnette*, 319 U.S. 624, 633-34 (1943).

Apple to provide assistance to FBI agents in their search of the shooter's cellular telephone, Apple make: iPhone 5c, Model: A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI: 358820052301414 on the Verizon Network.¹¹⁰ The Government could not complete the search of the lawfully seized phone because it was incapable of accessing the encrypted content.¹¹¹ The FBI requested Apple's assistance in completing its search, but Apple declined to provide that assistance.¹¹² The Government was concerned because the encryption is a user determined, numeric passcode and if more than ten erroneous attempts at the passcode were made, the information on the device would have become permanently inaccessible.¹¹³ The Government claimed that, on previous occasions, Apple had helped to access data on its devices, when presented with an appropriate warrant.¹¹⁴

In its argument to the court, the Government relied on the All Writs Act, which provides that: "all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."¹¹⁵ The Act may be used when the following four conditions have been met: 1) there is an absence of alternative methods, and other judicial remedies are not available; 2) an independent basis for jurisdiction is present;¹¹⁶ 3) the use of the Act is necessary or appropriate in the aid of jurisdiction, and in the particular case;¹¹⁷ and 4) the usage is agreeable to the usages and principles of law.¹¹⁸ In general, the All Writs Act has been a revived, proven mechanism for the Government to gain access to the cellphones of individuals linked to domestic terrorism and narcotics investigations.¹¹⁹ The Government

¹¹⁰ *Ex Parte Application*, *supra* note 15, at 2.

¹¹¹ *Ex Parte Application*, *supra* note 15, at, at 3.

¹¹² *Ex Parte Application*, *supra* note 15, at, at 3-4.

¹¹³ *Ex Parte Application*, *supra* note 15, at 3-4.

¹¹⁴ *Ex Parte Application*, *supra* note 15, at 3-4.

¹¹⁵ 28 U.S.C. § 1651(a) (1949).

¹¹⁶ Dimitry D. Portnoi, *Resorting to Extraordinary Writs: How the All Writs Act Rises to Fill the Gaps in the Rights of Enemy Combatants*, 83 N.Y.U. L. REV. 293, 299-303 (2008) (emphasizing that the act will not create jurisdiction which must be present under 28 U.S.C § 1331, 1332 or 1367).

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ Oscar Raymundo, *Here's a Map of Where Apple and Google are Fighting the All Writs Act Nationwide*, MACWORLD (Mar. 30, 2016),

then made an extensive argument explaining why the motion to compel should be granted under the All Writs Act.¹²⁰ More specifically, the Government requested that Apple create software to turn off the “auto erase” function on the iPhone to allow the entry of unlimited test passcodes until the correct combination could be pinpointed.¹²¹ The Government also insisted that the four conditions had been met because “the specific assistance sought can *only* be provided by Apple.”¹²²

The court granted the Government’s motion to compel on February 16, 2016, but invited Apple to make an application to the court for relief if “the order would be unreasonably burdensome.”¹²³ Apple informed the court that it would seek relief from the court order and a hearing was set for March 22, 2016.¹²⁴ On February 25, 2016, Apple filed a motion to vacate the order compelling its assistance.¹²⁵ Apple argued that the order would violate the First Amendment because it compelled Apple to write specific software, which is computer code protected under the First Amendment.¹²⁶ Relying on *Riley v. Nat’l Fed. of the Blind of N.C., Inc.*,¹²⁷ where the Court found that the Government’s compelling of speech triggered First Amendment protections,¹²⁸ Apple argued that compelled speech can only escape First Amendment protection if “it is narrowly tailored to obtain a compelling state interest”¹²⁹ and that the Government did not

<http://www.macworld.com/article/3049994/security/heres-a-map-of-where-apple-and-google-are-fighting-the-all-writs-act-nationwide.html>.

¹²⁰ *Ex Parte Application*, *supra* note 15, at 9-13.

¹²¹ *Ex Parte Application*, *supra* note 15, at 3-4.

¹²² *Ex Parte Application*, *supra* note 15, at 5.

¹²³ *Order Compelling*, *supra* note 105, at 3.

¹²⁴ Scheduling Order at 2, In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 15-0451M (9th Cir. 2016).

¹²⁵ *Motion to Vacate*, *supra* note 106.

¹²⁶ U.S. CONST. amend. I; U.S. CONST. amend IV; *Motion to Vacate*, *supra* note 106, at 32-33; *Universal City Studios, Inc.*, 273 F.3d at 449-51; *Junger*, 209 F.3d at 485; 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1099-1100 (N.D. Cal. 2004); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1126 (N.D. Cal. 2002); *Bernstein v. Dep’t of State*, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996).

¹²⁷ 487 U.S. 781 (1988).

¹²⁸ *Riley*, 487 U.S. at 796 (1988); *Motion to Vacate*, *supra* note 106, at 32.

¹²⁹ See *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 653 (1994); *Motion to Vacate*, *supra* note 106, at 32-33.

satisfy this standard, because it was only speculating as to the information contained on the device.¹³⁰ Apple further argued that

conscripting a private party with an extraordinarily attenuated connection to the crime to do the Government's bidding in a way that is statutorily unauthorized, highly burdensome, and contrary to the party's core principles, violates Apple's substantive due process right to be free from 'arbitrary deprivation of [its] liberty by Government.'¹³¹

Courts have constantly emphasized and recognized that "[t]he touchstone of due process is protection of the individual against arbitrary action of Government, . . . [including] the exercise of power without any reasonable justification in the service of a legitimate governmental objective."¹³² Essentially, Apple was concerned that the Order violated its due process rights and that the Government was overstepping its power in regard to Apple's privacy, extending it further than it constitutionally had the right to do.¹³³

B. In Support of Apple

Many aligned with Apple. To begin, AT&T Mobility LLC (hereinafter "AT&T") submitted an amicus brief.¹³⁴ AT&T justified this decision because "AT&T customers entrust it with some of their most personal and sensitive information" and, because of this commitment, want to protect that information from "intrusion or attack."¹³⁵ AT&T agreed that the court should not resolve this issue but, rather, Congress should pass legislation providing clear rules for companies and citizens.¹³⁶ Intel Corporations (hereinafter "Intel") also filed an amicus brief and delved into the potential global ramifications that may result if the Government were to affirmatively compel Apple

¹³⁰ *Motion to Vacate*, *supra* note 106, at 33.

¹³¹ *Motion to Vacate*, *supra* note 106, at 34.

¹³² *See* *Cnty. of Sacramento v. Lewis*, 523 U.S. 833, 845-46 (1998); *Costanich v. Dep't of Soc. & Health Servs.*, 627 F.3d 1101, 1110 (9th Cir. 2010) (citation omitted).

¹³³ *Motion to Vacate*, *supra* note 106, at 34.

¹³⁴ Brief of Amicus Curiae AT&T Mobility LLC in Support of Apple, Inc. at 1, In *Re* The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter "*Brief of AT&T*"].

¹³⁵ *Id.*

¹³⁶ *Id.* at 23.

to undermine its own software.¹³⁷ The dangers include setting a precedent to allow other courts to compel technological companies to comply with similar requests.¹³⁸ It would also force companies to create excessive technology to enable the companies to bypass their own security systems.¹³⁹ This would weaken security of devices while repressing innovation.¹⁴⁰

In addition, thirty-two law professors filed a brief in support of Apple, arguing that the Government went to great lengths to sidestep due process, as required by the Fifth and Fourteenth Amendments, in a struggle “to avoid judicial scrutiny of the merits of the case.”¹⁴¹ They asserted that the case lacked merit,¹⁴² insisting that “compelling a private company to create technology with features that the firm deliberately chose to exclude is an unprecedented expansion of judicial powers that Congress did not support by passing the All Writs Act.”¹⁴³ Furthermore, they firmly believed that the *ex parte* order violated Apple’s due process rights by depriving it of a hearing on the issue of burdensomeness prior to compelling the company to provide assistance to the Government.¹⁴⁴

The professors went on to argue that it is well-settled that in determining whether deprivation of due process is appropriate, a court must determine:

- (1) the importance of the individual’s interest at stake;
- (2) the likelihood that more formalized procedures would avoid arbitrary or erroneous decisions by the

¹³⁷ Notice of Motion and Motion of Intel Corporation for Leave to File as Amicus Curiae at ii, In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016); Brief of Intel Corporation as Amicus Curiae in Support of Apple, Inc., In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter “*Brief of Intel*”].

¹³⁸ *Brief of Intel*, *supra* note 137, at 11-12.

¹³⁹ *Brief of Intel*, *supra* note 137, at 12.

¹⁴⁰ *Brief of Intel*, *supra* note 137, at 12.

¹⁴¹ U.S. CONST. amend. V; U.S. CONST. amend. XIV; Amicus Curiae Brief of Law Professors in Support of Apple, Inc. at 1, In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter “*Law Professors’ Brief*”].

¹⁴² *Law Professor’s Brief*, *supra* note 141, at 1.

¹⁴³ *Law Professor’s Brief*, *supra* note 141, at 2.

¹⁴⁴ *Law Professor’s Brief*, *supra* note 141, at 5.

Government; and (3) the countervailing Government interest.¹⁴⁵

In determining whether the second prong was satisfied, the amici argued that by issuing the February 16th Order without hearing from Apple, the court made its decisions with incomplete information.¹⁴⁶ The Government, on the other hand, argued that the order did not place an “unreasonable burden” on Apple because the order . . . requires Apple to provide modified software [I]t is not an unreasonable burden for a company that writes software code as part of its regular business.”¹⁴⁷

In response, the professors pointed out that based on the same logic it would be unreasonably burdensome to require Boeing to “build a custom jet for the Government because Boeing builds planes as part of its regular business or to demand that a pharmaceutical company make drugs for executions after it has made the intentional decision not to.”¹⁴⁸ After a briefing from Apple, the professors asserted the court may consider the burden placed on Apple during developing, testing, and implementing the software, while preventing inappropriate individuals from obtaining the custom code created for the Government investigation.¹⁴⁹ In sum, the amici argued that, by not holding a hearing before entering the *ex parte* order, the court violated Apple’s right to due process.¹⁵⁰

Next, Air BNB, Atlassian, CloudFlare, eBay, GitHub, Kickstarter, LinkedIn, Mapbox, Medium, Meetup, Reddit, Square, Squarespace, Twilio, Twitter and Wickr submitted an amicus brief in support of Apple.¹⁵¹ In their brief, amici underscored how, in this era of rapid technological change, privacy is more important than ever before.¹⁵² They went on to explain that the smartphone touches every

¹⁴⁵ Mathews v. Eldridge, 424 U.S. 319, 321 (1976); *Law Professors’ Brief*, *supra* note 141, at 5.

¹⁴⁶ *Law Professor’s Brief*, *supra* note 141, at 6.

¹⁴⁷ *Law Professor’s Brief*, *supra* note 141, at 6; *Ex Parte Application*, *supra* note 15, at 17.

¹⁴⁸ *Law Professors’ Brief*, *supra* note 141, at 6.

¹⁴⁹ *Law Professors’ Brief*, *supra* note 141, at 6.

¹⁵⁰ *Law Professors’ Brief*, *supra* note 141, at 5.

¹⁵¹ Brief of Amici Curiae Airbnb, Inc. et al. at 5-6, In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) (arguing that allowing the government to force companies to undermine their own promised security measures will erode the core values of privacy) [hereinafter “*Brief of Airbnb*”].

¹⁵² *Id.* at 2.

aspect of modern life, as these devices provide endless services to an ever-growing populace.¹⁵³ The immense amount of information used, communicated, and stored digitally on the internet and on electronic devices “means that ‘privacy’ which ‘has been at the heart of democracy from its inception’ is ‘needed now more than ever.’”¹⁵⁴ Courts have often recognized that as technology develops and advances, the expectation of user privacy becomes heightened, not reduced.¹⁵⁵

In addition, the amici argued that a company’s protection of customer data is necessary to protect users from hackers and other criminal elements that threaten users of smartphones.¹⁵⁶ These companies disclose to their users how data may be divulged in certain circumstances and attempt to give their users this information in advance to demonstrate the importance of the principles of privacy and transparency.¹⁵⁷

Next, in an amicus brief filed by Amazon, Box, Cisco, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, and Yahoo, in support of Apple, the companies argued that, should the Government prevail, it would undermine the security of Americans’ most sensitive data.¹⁵⁸ These companies noted their lack of sympathy for terrorists and their response under the Stored Communications Act¹⁵⁹ to tens of thousands of lawful requests for customer data alone in the first six months of 2015.¹⁶⁰ But, they argued, the Government has urged these companies to combat trade-secret theft with increased security and encryption, making it very puzzling for the Government to now ask Apple to undermine its own security measures.¹⁶¹ Further, and even more

¹⁵³ *Id.* at 4.

¹⁵⁴ *Id.* at 6-7.

¹⁵⁵ *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (en banc) (“technology has the dual and conflicting capability to decrease privacy and augment the expectation of privacy.”); *Brief of Airbnb*, *supra* note 151, at 6-7.

¹⁵⁶ *Brief of Airbnb*, *supra* note 151, at 5.

¹⁵⁷ *Brief of Airbnb*, *supra* note 151, at 8.

¹⁵⁸ *Brief of Amici Curiae Amazon.com et al.*, at 3, *In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203*, No. ED 15-0451M (9th Cir. 2016) [hereinafter “*Brief of Amazon.com*”].

¹⁵⁹ 18 U.S.C. § 2701 (2002).

¹⁶⁰ *Brief of Amazon.com*, *supra* note 158, at 4.

¹⁶¹ *Brief of Amazon.com*, *supra* note 158, at 18; *Administration Strategy on Mitigation the Theft of U.S. Trade Secrets*, THE UNITED STATES DEPARTMENT OF JUSTICE (Feb. 2013), <https://www.justice.gov/criminal-ccips/file/938321/download>.

disconcerting, the amici observed that the Federal Trade Commission has threatened to sanction companies that do not adequately secure their customers' data.¹⁶²

These companies recognized that a lawful warrant will force the handing over of data, "but once a company builds a security-defeating tool, it cannot guarantee that it will be used by law enforcement only."¹⁶³ One legislator explained that if backdoors are put in place for the convenience of the Government, then those backdoors could be exploited by hackers as well.¹⁶⁴ The Government may believe that the benefits to its investigation substantially outweigh the risk to the companies, but "the All Writs Act does not authorize a court to order a party to bear risks not otherwise demanded by law, or to aid the Government in conducting a more efficient investigation."¹⁶⁵ Further, amici argued that compelling Apple to write the software violates its freedom of speech, a term that comprises both the decision of what to say and what not to say.¹⁶⁶ Therefore, Apple's code is protected speech because it has long been held that software is speech, and that technology companies have the right to decide what *not* to say.¹⁶⁷

Finally, Lavabit submitted a brief in support of Apple, citing that it is in an "unusually helpful position to serve as amicus curiae because it too was compelled to provide extraordinary assistance to the Government" in 2013.¹⁶⁸ The brief argued that the Government's request violated Apple's freedom of speech guaranteed by the First Amendment and equated this request with involuntary servitude.¹⁶⁹ Although Apple is a corporation, it has the same rights as an individual and should not be required to provide speech that "contravenes its fundamental beliefs that is, the belief that its customers should have

¹⁶² FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240-42 (3d Cir. 2015); *Brief of Amazon.com*, *supra* note 158, at 18.

¹⁶³ *Brief of Amazon.com*, *supra* note 158, at 20.

¹⁶⁴ *Brief of Amazon.com*, *supra* note 158, at 20; Erin Kelly, *Bill Would Stop Feds from Mandating 'Backdoor' to Data*, USA TODAY (Apr. 2 2015), <http://www.usatoday.com/story/news/politics/2015/04/02/encryption-bill-tech-companies-federal-law-enforcement/70734646/> (quoting Representative Thomas Massie).

¹⁶⁵ *Brief of Amazon.com*, *supra* note 158, at 21.

¹⁶⁶ *Brief of Amazon.com*, *supra* note 158, at 23.

¹⁶⁷ *Riley*, 487 U.S. at 796-97; *Brief of Amazon.com*, *supra* note 158, at 23.

¹⁶⁸ *Brief of Amicus Curiae Lavabit LLC in Support of Apple Inc.'s Motion to Vacate at 4, In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016).*

¹⁶⁹ *Id.* at 12-13.

the highest level of security and privacy in their personal data.”¹⁷⁰ Lavabit urged the Government to take steps towards protecting electronic privacy, rather than weakening it.¹⁷¹

C. In Support of the FBI

Greg Clayborn, James Godoy, Hall Houser, Tina Meins, Mark Sandefur and Robert Velasco submitted an amicus brief to the court in support of the FBI and its motion to compel.¹⁷² These amici curiae are close relatives of those murdered in the attack in San Bernardino.¹⁷³ The amici argued that this case presented no threat to the individual’s privacy rights and involved no intrusion into any cognizable privacy right,¹⁷⁴ reasoning that the iPhone was seized by search warrant and, under the American system of laws, one does not enjoy the privacy to commit crimes.¹⁷⁵ Moreover, they claimed that, because San Bernardino County owns the phone, and made this request together with law enforcement, this case did not implicate privacy concerns.¹⁷⁶

Also in support of the petitioner, the San Bernardino County District Attorney (hereinafter “DA”) submitted an amicus brief.¹⁷⁷ The DA asserted that Apple lacked standing to challenge the issue of privacy,¹⁷⁸ insisting that privacy is a personal right that cannot be asserted by third parties.¹⁷⁹ He also contended that Apple’s general pronouncement of privacy did not give a right to privacy to the iPhone in question.¹⁸⁰ “The concept of absolute privacy bolstered by the technology deployed by Apple is not a legally-cognizable precept, and is not sufficient to overcome the compelling Government interests in

¹⁷⁰ *Id.*

¹⁷¹ *Id.* at 18.

¹⁷² Amicus Curiae Brief of Greg Clayborn et al., In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter “*Brief of Clayborn*”].

¹⁷³ *Id.* at 1.

¹⁷⁴ *Id.* at 4.

¹⁷⁵ See *Virginia v. Moore*, 553 U.S. 164, 171 (2008); *Kolender v. Lawison*, 461 U.S. 352, 369 n.7 (1983); *Brief of Clayborn*, *supra* note 171, at 5.

¹⁷⁶ *Brief of Clayborn*, *supra* note 171, at 6.

¹⁷⁷ San Bernardino County District Attorney Amicus Curiae Brief in Support of The United States Government, In Re The Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M (9th Cir. 2016) [hereinafter “*Brief of DA*”].

¹⁷⁸ *Id.* at 7-9.

¹⁷⁹ *Id.* at 9.

¹⁸⁰ *Id.*

acquiring the evidence contained on the seized iPhone.”¹⁸¹ Furthermore, the DA argued that it is appropriate for Apple to remedy this problem which it created.¹⁸² The Government and the county were not particular about the method Apple chose or whether it merely turned over the tool it used to override the encryption,¹⁸³ but asked the court to compel Apple to override the encryption so that they may obtain the information necessary to prosecute the crime.¹⁸⁴

III. ANALYSIS

To begin, Apple would have suffered irreparable harm if it had granted the Government the relief it sought. When Apple chose not to fully comply with the Order, the issue for the company was whether a right to privacy should be applied to the data stored on an iPhone. A comparison to the *Lavabit* case is instructive. Although the *Lavabit* case has been sealed, the Government was given unhindered access to the users’ emails.¹⁸⁵ Should the Government be afforded the same access to encrypted data on iPhone users’ phones, the public outrage would certainly be comparable, and probably greater. *Lavabit* was also forced to cease doing business after the case was brought to public attention because users no longer trusted an insecure network to host their emails.¹⁸⁶ Had Apple’s order been sealed as in *Lavabit*, and had Apple not received media attention and subsequent support and amicus briefs from other tech moguls, it may have met a similar fate.¹⁸⁷ Consequently, the harm suffered by *Lavabit* would likely have been inflicted upon, and simply not have been sustainable by, Apple.

Furthermore, there is reason to believe that, if this matter were to reach Supreme Court, Apple would be successful. The test for a reasonable privacy expectation, as outlined in *Katz*, can be satisfied by showing that there is an expectation that a barrier to prevent arbitrary governmental intrusion on one’s smartphone exists, and that society is prepared to recognize this expectation as reasonable.¹⁸⁸ Indeed, the

¹⁸¹ *Id.* at 9.

¹⁸² *Brief of DA, supra* note 176, at 11.

¹⁸³ *Brief of DA, supra* note 176, at 11.

¹⁸⁴ *Brief of DA, supra* note 176, at 11.

¹⁸⁵ *Ciobotea, supra* note 24.

¹⁸⁶ *Ciobotea, supra* note 24.

¹⁸⁷ *Ciobotea, supra* note 24.

¹⁸⁸ *Katz*, 389 U.S. at 367.

amicus briefs in support of Apple demonstrate that this expectation exists.¹⁸⁹ Further, public outrage after Snowden's revelation of governmental intrusion on the Lavabit server demonstrates that there is a definite public expectation that electronic information retained on electronic devices or servers are owed a more substantial degree of privacy than currently recognized by the courts.¹⁹⁰

In addition, the holding in *Centennial Insurance Co.*, where the court found that computer data could potentially be regarded as tangible property,¹⁹¹ would expand the Fourth Amendment to apply to computer data retained on a smartphone. This issue would be one of first impression for the Supreme Court, but, one could speculate that similar to *Retail Systems*, where the data was deemed to be merged with the device itself, and thus existed as tangible property, the data contained on an iPhone could be merged with the device itself and thus be protected under the Fourth Amendment.¹⁹²

Moreover, analysts have demonstrated that a growing number of people believe that the protection of personal data is a fundamental civil liberty interest.¹⁹³ Fundamental liberty interests have been defined by the Supreme Court to mean liberties that are "principle[s] of justice so rooted in the traditions and conscience of our people as to be ranked as fundamental" and are entitled to protection from governmental intrusions.¹⁹⁴ The right to privacy for data contained on smartphones cannot be explicitly deeply rooted in our nation's history and tradition, as they are a recent phenomenon that continues to develop.¹⁹⁵ The Court is tasked with determining which rights are fundamental and thus subject to greater protection against governmental intrusions. As personal data protection is viewed as

¹⁸⁹ See *Brief of AT&T*, *supra* note 134; *Brief of Intel*, *supra* note 137; *Law Professors' Brief*, *supra* note 140; *Brief of Airbnb*, *supra* note 151; *Brief of Amazon.com*, *supra* note 158.

¹⁹⁰ *Ciobotea*, *supra* note 24.

¹⁹¹ *Centennial Insurance Co.*, 710 F.2d at 1292 (holding that tangible property is an ambiguous term in insurance policies and that when addressed by a court, the court would need to determine how the Fourth Amendment would apply).

¹⁹² *Retail Systems, Inc.*, 469 N.W.2d at 738.

¹⁹³ *Samuelson*, *supra* note 57.

¹⁹⁴ *Palko v. State of Conn.*, 302 U.S. 319, 325 (1937) (explaining that a liberty interest exists when something is so rooted in the traditions and conscience of the American people that it becomes fundamental).

¹⁹⁵ *Obergefell v. Hodges*, 135 S. Ct. 2584, 2618 (2015) (discussing importance of marriage to society and reaffirming that the right to marry is fundamental, expanding what traditional marriage meant and applying it to same sex marriage); *Roe v. Wade*, 410 U.S. 113, 151-54 (1971) (viewing abortion as a fundamental right that was not absolute, but qualified).

essential to individual autonomy and freedom, it is likely that the Court will find a liberty interest to be present.¹⁹⁶

Furthermore, a statute such as 18 U.S.C. § 1702 exists to prevent the opening, meddling, or prying of information from mail addressed to someone other than the person opening the mail.¹⁹⁷ The intent of the drafters of this law can be juxtaposed with the intent of those proposing a privacy right over personal data contained in digital format.¹⁹⁸ The intention of this law is to protect mail from interference by an unauthorized third party.¹⁹⁹ While the use of ‘snail-mail’ has decreased in popularity, the use of electronic mail and text messaging has skyrocketed.²⁰⁰ It is therefore reasonable for citizens to anticipate the same protection from interference with digital communications as they have come to expect with written snail-mail.

Finally, with regard to the free speech issue raised under the First Amendment, this case can be compared to *Suarez v. Trigg Laboratories, Inc.*²⁰¹ The court’s finding in *Suarez* protects a speaker’s right to *withhold* and *refrain* from speech.²⁰² Similarly, courts should protect Apple’s right *not* to create code for the Government. As source and object code has been deemed speech subject to First Amendment protection, it is important the Government protect this important right of a large corporation as it would for an individual.²⁰³ Here, when the court granted the FBI’s motion to compel, it was essentially compelling Apple to speak, in the form of creating code, against its will.²⁰⁴ It was this hesitation that compelled Apple to oppose the order, because being forced to speak when Apple explicitly did not wish to speak, was believed to be a blatant violation

¹⁹⁶ Samuelson, *supra* note 57.

¹⁹⁷ 18 U.S.C. § 1702 (1994).

¹⁹⁸ 18 U.S.C. § 1702 (1994).

¹⁹⁹ 18 U.S.C. § 1702 (1994).

²⁰⁰ Randolph E. Schmid, *You Never Write Anymore? Well Hardly Anyone Does*, NBC News (Oct 3, 2011), http://www.nbcnews.com/id/44760552/ns/technology_and_science-tech_and_gadgets/t/you-never-write-any-more-well-hardly-anyone-does/#.WMxeQVffTvw; Adam Hartung, *Why The Postal service Is Going out of Business*, FORBES (Dec. 6, 2011), <https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/adamhartung/2011/12/06/why-the-postal-service-is-going-out-of-business/&refURL=https://www.google.ca/&referrer=https://www.google.ca/>; Chris Crum, *Is Email Killing The Post Office?*, WEBPRONEWS (May 29, 2011), <http://www.webpronews.com/email-post-office-2011-05/>.

²⁰¹ *Suarez*, 3 Cal. App. 5th at 118.

²⁰² *Id.* at 124.

²⁰³ Samuelson, *supra* note 57

²⁰⁴ *Motion to Vacate*, *supra* note 106, at 34.

of the First Amendment.²⁰⁵ The right to be protected from compelled speech is paramount in American democracy and if the Government starts mandating and compelling the speech of corporations, the First Amendment will be infringed.²⁰⁶ In this area, it is important for the Court to follow prior decisions and respect *stare decisis*, conferring protection for computer code.²⁰⁷

III. CONCLUSION

Had *In Re The Search of an Apple iPhone* advanced to be heard by the court, it would have been a difficult determination to balance the FBI's and Apple's interests. As constitutional infringements create a slippery slope, a court should be hesitant when considering extending limitations beyond those of the Constitution. It is likely that the Supreme Court would find in Apple's favor. Apple should not have been required to turn over the software because: (1) an individual's right to privacy with regard to a smartphone exists and should be recognized by the Court; and (2) speech in the form of computer code should be afforded constitutional protection under the First Amendment as it has been classified as speech in prior Supreme Court decisions. Although this matter did not reach a judicial resolution as the FBI withdrew its motion, it is a matter of time before an issue of this kind will emerge before the bench, and the Supreme Court will be required to decide where the axiomatic line in the sand should be drawn.

²⁰⁵ *Motion to Vacate*, *supra* note 106, at 34.

²⁰⁶ U.S. CONST, amend. I.

²⁰⁷ See Margaret N. Kniffen, *Overruling Supreme Court Precedents: Anticipatory Action by The United States Courts of Appeals*, 51 *FORDHAM L. REV.* 53 (1982) (following *stare decisis*, the doctrine looking at precedent, or past legal decisions on the same issue, is not required of the Supreme Court as it is of lower courts, but is often done).